ANÁLISIS Y DISEÑO DE UNA SOLUCIÓN DE SEGURIDAD PARA EL CONTROL DE ACCESOS ENFOCADOS EN LA IBNS SOBRE LA INFRAESTRUCTURA TECNOLÓGICA DE UNA EMPRESA FINANCIERA Y DE SERVICIOS

Lescano Rodríguez Daniel Martín

Escuela Politécnica del Ejército
Sangolquí – Ecuador

Resumen

El proyecto denominado Análisis y Diseño de una Solución de Seguridad para el Control de Accesos Enfocados en la IBNS Sobre la Infraestructura Tecnológica de una Empresa Financiera y de Servicios, tiene como objetivo fundamental forjar un mecanismo de seguridad en la infraestructura tecnológica de una empresa financiera y de servicios; dado que en este tipo de instituciones se maneja gran cantidad de dinero, es necesario contar con un mayor control de acceso a la red, ya sea esto en caso de fuga de información o de personal no autorizado que quiera ingresar a la red de la entidad.

Para esto se optó por la Identidad Basada en Servicios de Red (IBNS), la cual utiliza un servidor AAA, el mismo que se encarga de la autenticación, autorización y *accounting* (registro), para que los funcionarios de la institución financiera, puedan ingresar a la red y desarrollar su desempeño laboral con sus respectivos roles y perfiles sin tener ningún inconveniente.

El servidor AAA, se enlazará con una base de datos, ya sea esta externa o interna, y el equipamiento requerido para que esto se encuentre acorde a la configuración y funcionamiento apropiado.

En el resultado de este proyecto, se obtuvo un mayor control en el acceso a la red de la institución ya que exclusivamente los usuarios que pertenezcan a la institución, van a poder ingresar a la infraestructura tecnológica de la misma.

1. Introducción

La Identidad Basada en Servicios de Red, ofrece un sistema de control centralizado en el acceso a la red, gestionado por medio de un servidor de autenticación AAA/ACS y los protocolos RADIUS y TACACS, dado que con estos se puede determinar la funcionalidad, protocolo de transporte y soporte, dirección, confidencialidad y registro, los mismos que pueden ofrecen el aumento de la productividad, y ofrece las interacciones con clientes.

El ACS es un servidor de seguridad basado en políticas que provee Autenticación Autorización y *Accounting* o registro (AAA). Además el manejo de protocolos estándar para la administración de seguridad basada en identidad, tanto de equipamiento como de usuarios.

El servidor de autenticación es una plataforma robusta para el control de acceso a la red en base a la identidad, que proporciona un modelo de políticas basadas en los roles y perfiles de cada cargo de los funcionario de la institución, fundado en condiciones dinámicas y atributos.

El modelo de políticas basadas en reglas, está diseñado para satisfacer necesidades de políticas de acceso complejas.

En el marco del protocolo RADIUS, el ACS permite el control de acceso por cable e inalámbrico de los usuarios y host a la red así como administra el accounting de los usuarios que ingresan a la infraestructura tecnológica.

Mientras que el protocolo TACACS, permite y simplifica la administración basado en identidad de equipos y fabricantes.

dani_filth2@hotmail.com

2. Identidad Basada en Servicios de Red (IBNS)

La IBNS es una solución unificada de Cisco que incluye varios dispositivos para permitir la autenticación, control de acceso y aplicación de políticas de usuarios (basados en identidad) para acceder de forma segura (conectividad) a la red y sus recursos.

Además permite a las empresas el manejo seguro de la movilidad de sus empleados (acceso remoto), como la asignación de los usuarios a su correspondiente segmento de red basados en su identidad.

Figura 1. Ingreso basado en IBNS de Cisco

3. Servidor AAA

El servidor AAA es un servidor de Autenticación (AAA/ACS), el mismo que realiza la autenticación, autorización y accounting o registro para la validación de identidad del usuario (sea en la base de datos interna o en una base de datos externa como el Directorio Activo o LDAP) y notifica al Switch/WLC si el cliente está autorizado para acceder a la LAN y a los servicios del intermediador, siendo el intermediador un cliente RADIUS del ACS.

El protocolo RADIUS lleva a la autenticación, autorización e información de configuración entre un *Network Attached Storage* (NAS) y un servidor RADIUS de autenticación.

Las solicitudes y respuestas realizadas por el protocolo RADIUS se llaman atributos de RADIUS. Estos atributos pueden ser nombre de usuario, tipo de servicio, y así sucesivamente, además proporcionan la información necesaria para un servidor RADIUS para autenticar a los usuarios y para establecer el servicio de red autorizado por ellos. El protocolo RADIUS también lleva la información contable entre un NAS y un servidor RADIUS de contabilidad.

El funcionamiento del servidor AAA, se establece mediante los parámetros de autenticación, autorización y *accounting*.

Autenticación: los funcionarios deben probar que son ellos mediante usuario y contraseña, cuestiones desafío-recontraseña, cuestiones desafío-respuesta, tokens. Hace referencia a quien es permitido el acceso a la red.

Autorización: determina a Autorización: determina a que recursos puede acceder un usuario después de haberse autenticado.

Accounting (registro): que acciones han realizado los usuarios mientras se encontraban en la red.

Mediante el *accounting* se recogen datos que pueden ser utilizados en auditorias o para la elaboración de facturas, estos datos incluyen horas de comienzo y fin.

4. IEEE 802.1x

Para el control de acceso a la red, se establece con el protocolo de la IEEE 802.1x. Este tipo de protocolo, permite la autenticación de los clientes conectados a los puertos LAN al switch, permitiendo o no el acceso a la red (habilitando o no el puerto en base al estado de la autenticación).

Los componentes que constituyen la solución de seguridad en el acceso a la red de la institución en relación con INBS son:

- **Cliente.-** Host (Estación de Trabajo con funcionalidades 802.1x) que envía requerimientos de acceso a la LAN/Switch/WLC y responde a los requests del Switch/WLC.

- **Inermediador**.- Switch de acceso, Access Point o Wireless LAN Controller que controla el acceso físico a la red basado en el estado de autenticación del cliente, estos dispositivos actúan como un intermediador entre el cliente y el servidor de autenticación AAA/ACS.

- **Servidor AAA.-** realiza la autenticación, valida la identidad del cliente (sea en una BDD interna o externa como Active Directory) y notifica al Switch/WLC si el cliente está autorizado para acceder a la LAN y a los servicios del intermediador, siendo el intermediador un cliente Radius del ACS.

- **Directorio Activo**.- Base de datos externa.

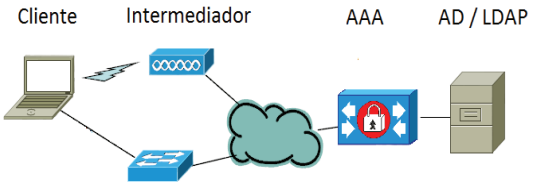

Figura 2. Componentes de IBNS de Cisco

La autenticación se basa en un Protocolo Extensible de Autenticación (EAP).

El EAP es un framework de autenticación utilizada tanto en redes WLAN como en LAN cableadas, además es una estructura de soporte que no define un único mecanismo de autenticación, sin embargo provee un conjunto de funcionalidades comunes para el o los mecanismos de autenticación escogidos; estos mecanismos se los conoce como métodos EAP.

El PEAP utiliza Transport Layer Security (TLS) para formar un túnel cifrado entre el intermediador (ej.switch) y un servidor de autenticación (ej.ACS), PEAP no define un método de autenticación sino que provee encapsulación segura (túnel cifrado) para transporte del método EAP.

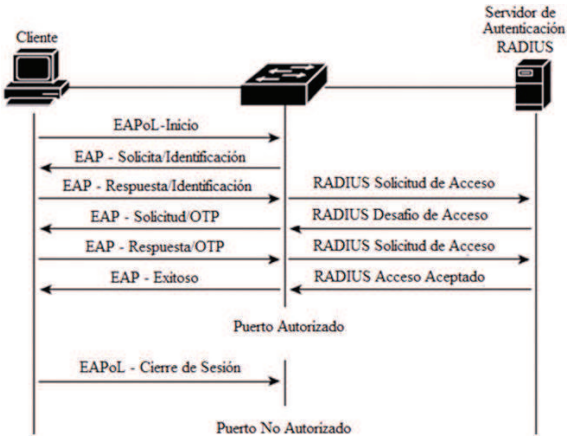

Figura 3. Intercambio de Mensajes

5. Configuración de ACS

Debemos iniciar la configuración mediante un emulador de terminal (Hyper Terminal) con los siguientes parámetros.

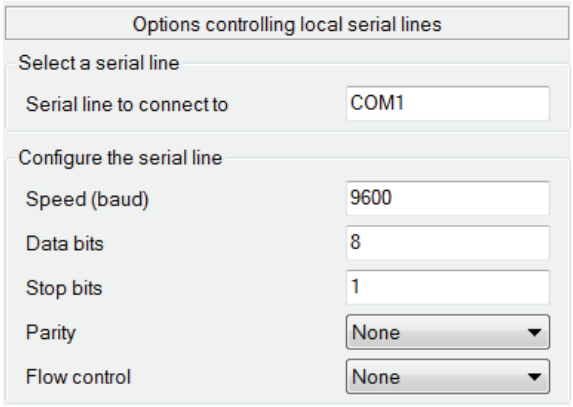

Figura 4. Hyper Terminal

En la consola de administración (CLI) nos aparecerá un mensaje “localhost login:”, en el cual ingresamos “setup”.

Figura 5. Mensaje localhost login

Ingresamos los datos requeridos en el proceso de instalación.

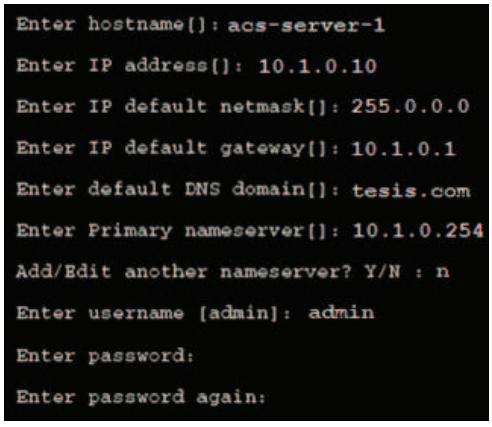

Figura 6. Proceso de instalación ACS

Ingresamos a la interfaz gráfica de administración mediante un web browser con la siguiente url:

- https://<acs_host>/acsadmin,

Donde <acs_host> es la dirección IP del equipo.

Ingresamos las credenciales por defecto:

- **Username:** ACSAdmin y **Pasword:** default

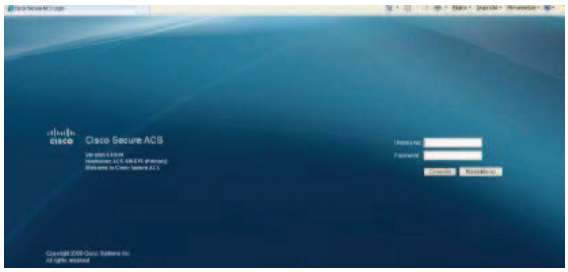

Figura 7. Interfaz gráfica

A continuación se solicitará el cambio de la contraseña. Tras realizar el cambio de la contraseña se ingresará a la página principal de la interfaz gráfica de Administración y Configuración.

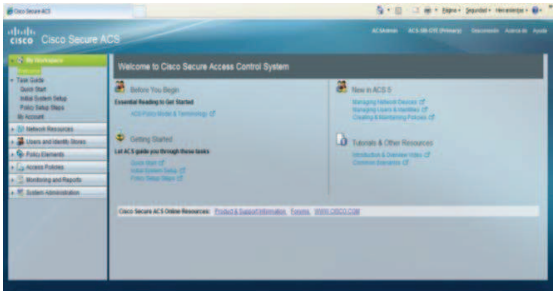

Figura 8. Página principal ACS

6. Configuración de los Dispositivos de Acceso a la Red

En esta sección se ingresa al ACS los dispositivos de red (intermediadores switch, routers, otros) pudiendo ser estos clientes RADIUS o TACACS+.

Ingresamos a la pestaña Network Resources, seleccionamos Network Device Groups para definir los tipos de dispositivos y sus ubicaciones.

Figura 9. Localización y creación de usuarios

Ingresamos los datos solicitados para la ubicación (*Name, Description, Parent*)

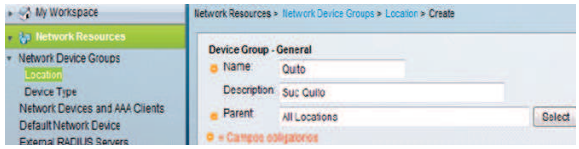

Figura 10. Datos de ingreso de ubicación

En la sección *Parent* se puede elegir la raíz de la estructura de ubicaciones para un manejo jerárquico de ubicaciones

Figura 11. Parámetros de acuerdo a la ubicación configurada

Visualizamos los parámetros configurados:

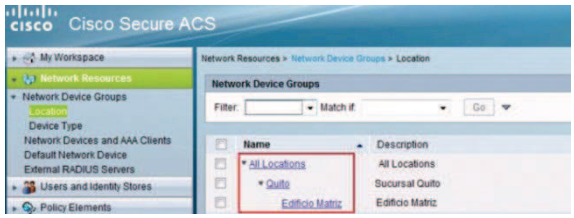

Figura 12. Visualización de parámetros configurados

Ingresamos los Tipos de Dispositivos en la Pestaña *Device Type*

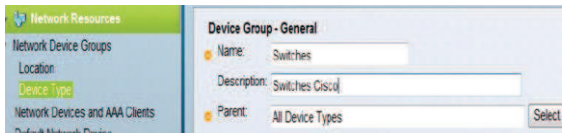

Figura 13. Ingreso de tipos de dispositivos

Visualizamos los Tipos de Dispositivos configurados (Pueden ser archivos .csv)

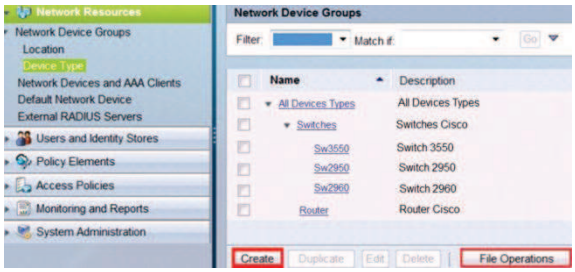

Figura 14. Visualización de dispositivos en ingreso .csv

Configuramos los dispositivos con los protocolos RADIUS y TACACS

Figura 15. Configuración de RADIUS Y TACACS

Visualizamos la configuración TACACS+ y RADIUS

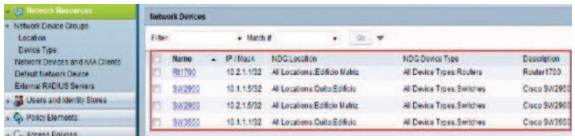

Figura 16. Visualización de configuración de RADIUS Y TACACS

7. Configuración de Repositorios

A través de la opción User and Identity Stores, el ACS puede administrar la base de datos (Interna o Externa) donde las credenciales (identidad) del cliente puedan ser validadas.

Cuando un cliente requiere acceso a la red sus credenciales son enviadas al ACS; para autenticar y autorizar al cliente, el ACS consulta las bases de datos creadas en *User and Identity Stores.*

Para la configuración de la BDD interna, ingresamos los parámetros requeridos como muestra la figura 16:

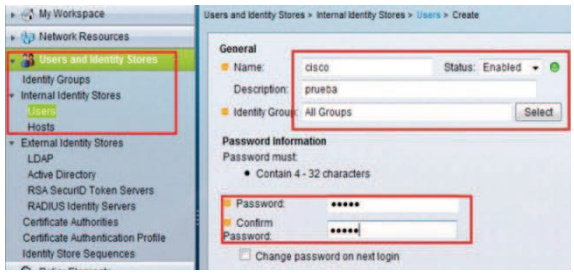

Figura 17. Ingreso de Datos (Name, Description, Parent y Password)

También podemos configurar una base de datos interna con la dirección MAC como muestra la siguiente figura:

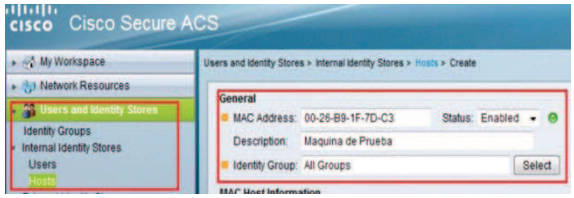

Figura 18. Configuración de la BDD interna (Dirección MAC)

Posteriormente visualizamos los host configurados.

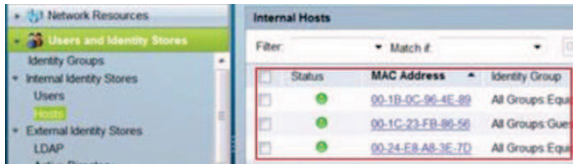

Figura 19. Visualización de la BDD interna (Dirección MAC)

Para la configuración de BDD externa, lo realizamos por medio del Directorio Activo.

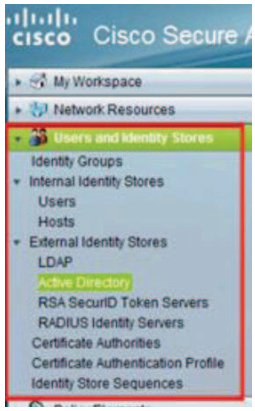

Figura 20. Configuración Directorio Activo

Ingresamos los datos solicitados (Nombre del Dominio, usuario y password de la cuenta con Ingresamos los datos solicitados (nombre del dominio, usuario y password de la cuenta con la que accederemos al directorio) y realizamos un Test de Conexión.

Figura 21. Ingresamos los parámetros requeridos (Directorio Activo)

Para la secuencia de búsqueda debemos seleccionar el orden de localización de las credenciales de los usuarios.

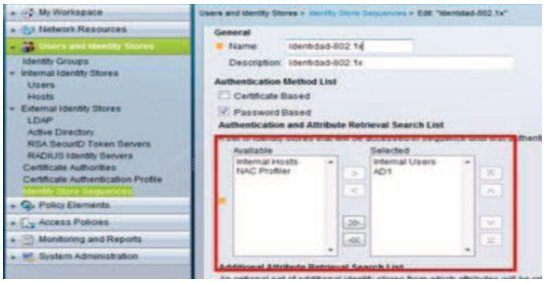

Figura 22. Secuencia de búsqueda

8. Configuración de VLAN's

Para realizar la configuración de VLAN's, procedemos a determinar que redes van a estar destinadas para cada uno de los cargos administrativos que tenga una institución.

Debemos tomar en cuenta que para este tipo de configuraciones, se opta por direcciones IP públicas por motivos de configuración.

Las VLAN's se encuentran determinadas de la siguiente manera:

VLAN Id	Descripción	Dirección de Red	Función
1	Administrativa	192.168.1.0 /24	Nativa
2	Directores	192.168.2.0 /24	Critical
3	Empleados	192.168.3.0 /24	
4	Invitados	192.168.4.0 /24	Guest

Tabla 1. Descripción de VLAN´s

A continuación ingresamos los datos solicitados para la creación de las VLANs de acuerdo a nuestro requerimiento.

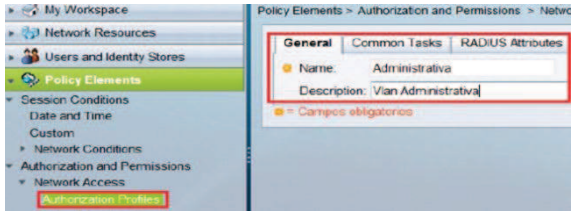

Figura 23. Configuración de VLAN´s

Para la creación de los perfiles ingresamos a la sección "User and Identity Stores/Internal Identity Store/User", seleccione "Create" e ingresamos los parámetros requeridos. Damos clic en *new* y se va a desplegar un nuevo usuario, en el cual se puede editar sus diferentes parámetros de acuerdo a nuestro requerimiento.

Figura 24. Configuración de perfiles

Posteriormente Obtendremos los nombres de perfiles configurados de la siguiente manera:

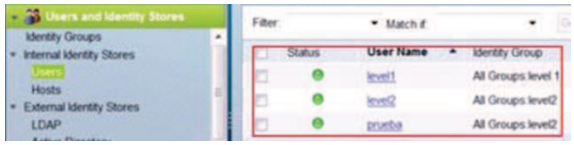

Figura 25. Visualización de perfiles

9. Reporte RADIUS y TACACS

Finalmente, podemos obtener un reporte tanto del protocolo RADIUS como TACACS, los mismos procedemos de un monitoreo en base a nuestra configuración.

Para proceder con los reportes, nos ubicamos en Monitoring and Reports/Dashboard como se observa en la siguiente figura:

Figura 26. Monitoreo y reportes

Posteriormente sacamos los reportes RADIUS y TACACS de acuerdo a nuestro requerimiento.

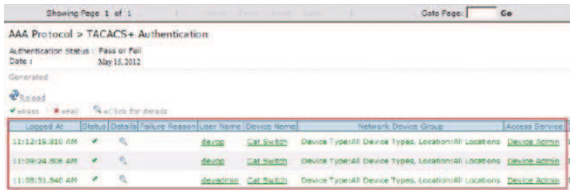

Figura 27. Reporte TACACS

Figura 28. Reporte RADIUS

10. Análisis de Costos

Para la estimación del costo del equipamiento enfocado en el servidor AAA de la red de la institución financiera, es importante contar con información de ofertas reales, las mismas que se van a encontrar en el mercado ecuatoriano.

Para esto estimamos la siguiente tabla con valores reales de equipamiento con los que se cuenta en la actualidad en el mercado ecuatoriano.

Nombre	Desarrollador	Cantidad	Precio Unitario	Valor
Switch WS-C2960-48TT-L	Cisco Catalyst	2	1048	2096
Switch WS-C3550G-48TS-S	Cisco Catalyst	2	3518	7036
Cisco Catalyst 2950G-48 Ethernet Switch	Cisco Catalyst	2	2150	4300
Cisco 1721 VPN Security Router Bundle	Cisco System	2	1798,74	3597,48
Servidor Windows	Windows	1	469,00	469,00
Materiales		500	0,75	375
Personal Capacitado		3	600	1800
			Sub-Total:	19673,48

Tabla 2. Costos de equipamiento compatible

Adicionando el costo del servidor AAA tenemos:

Descripción	Precio
Cisco Secure Access Control System (ACS)	14995
Sub-Total (Equipamiento Compatible)	19673,48
Total:	34668,48

Tabla 3. Costo total ACS y equipos

11. Análisis de Costo/Beneficio

- Se establece mediante el análisis de seguridad que los funcionarios no pretendan extraer información susceptible que a la larga pueda afectar a la institución.
- Un nuevo sistema de seguridad basado en el servidor de autenticación, le de acceso solamente a las funciones que estos servidores requieran para desarrollar su trabajo y no para el mal uso de la información a la que estos puedan acceder.
- Se maneja altas sumas de dinero.
- Manipulación de información institucional con fines de lucro.

12. Conclusiones y Recomendaciones

- El análisis y diseño de este proyecto, ayuda a tener una mejor proyección en los ambientes de control de acceso a la red de una institución financiera y a su vez establece una seguridad en el manejo de información.
- La seguridad que presta el servidor de autenticación es muy valiosa para instituciones que tienen información confidencial, ya que la mala utilización de la misma puede ser perjudicial para dicha entidad.
- El servidor AAA desempeña una barrera de seguridad mejor elaborada con un seguimiento exhaustivo del ingreso de los funcionarios a la red de la institución financiera. Además establece un óptimo sistema con el cual evita ataques y fraudes.

- El servidor AAA al ser un módulo centralizado, debe ser capaz de manejar todas las conexiones de la red de la institución financiera además de controlar el acceso a la red en todo momento.

- Al centralizarse todo el sistema con el servidor de autenticación, se logra obtener un manejo fácil del enlace, ya que se tiene todas las aplicaciones concentradas en un solo servicio y permite de esta manera una configuración más rápida y sencilla.

- La integración del servidor RADIUS con el control de tráfico y la base de datos, se alcanzó con el objetivo del diseño de la aplicación para la administración en base a un nivel de privilegios establecidos en el sistema de autentificación.

- La relación y enlace a cada rol y perfil de los funcionarios, se lo desarrolla mediante los roles y perfiles que cada institución los tengan, es decir, va a depender de la entidad en la que se desee desarrollar este sistema de autenticación ya que este análisis se lo realiza de manera general para cualquier organismo financiero sin importar la cantidad de roles y perfiles que tenga cada cargo.

- Se logró establecer un mecanismo de seguridad en el cual se detalle la autenticación, control y registro de cada uno de los funcionarios que ingresen a la red de la institución financiera.

- Se analizó el equipamiento compatible con el servidor AAA, ya que si se utiliza router o switches de otras marcas, que no sean del mismo servidor de autenticación, pueden traer problemas en el momento de su conexión.
- La configuración con los roles y perfiles de los cargos de los funcionarios, va a depender del Directorio Activo, ya que si este no funciona, el servidor AAA no logrará establecer los aplicativos a los cuales pertenece cada usuario.

- Solamente los funcionarios que se encuentren autorizados, podrán manipular y configurar el servidor AAA.

- Se debe establecer una ruta crítica en caso de controversias en las actividades, dado que se pueden encontrar problemas, ya sean estos de índole administrativa, financiero o al momento de su ejecución.

- Se debe tomar muy en cuenta las direcciones Ip con las que se vaya a trabajar, dado que son direcciones privadas y de carácter confidencial.

- Solamente los funcionarios que se encuentren autorizados, podrán manipular y configurar el servidor AAA.

- Establecer grupos de administradores para el servidor AAA con el fin de llevar a cabo la autenticación, autorización y administración de las cuentas de los funcionarios.

- Dado que el ACS es una solución unificada de Cisco, es recomendable la utilización de equipos de la misma marca.

13. Referencia de Figuras:

14. Referencia de Tablas:

- **Tabla 1.** Descripción de VLAN´s
- **Tabla 2.** Costos de equipamiento compatible
- **Tabla 3.** Costo total ACS y equipos

15. Bibliografía:

- Cisco Systems, Inc, *User Guide for the Cisco Secure Access Control System 5.1*, Americas Headquarters, 1ª ed., West Tasman Drive San Jose, CA 95134-1706 USA, Marzo 2009, 618.
- Cisco Systems, Inc, Catalyst 3750-E and 3560-E Switch Software Configuration Guide, 12 ª ed., Americas Headquarters, 170 West Tasman Drive San Jose, CA 95134-1706 USA, Marzo 2009, 1410.
- AREITO, Javier, Seguridad de la Información, Redes, Informática y Sistemas de Información, 1ª ed., PARANINFO, Magallanes, 25;28015 Madrid - España, 2008, 561
- http://www.cisco.com/en/US/products/ps6663/products_ios_protocol_option_home.html, Authentication, Authorization, and Accounting (AAA)
- http://www.cisco.com/en/US/products/ps6638/products_data_sheet09186a00804fe332.html, Authentication, Authorization, and Accounting (AAA)
- http://technet.microsoft.com/es-es/library/cc732681(WS.10).aspx, Protocolo de autorización de credenciales de host
- http://www.cisco.com/en/US/solutions/collateral/ns340/ns394/ns171/ns466/ns812/guide_c07-491729.html&ei=KNY2TuTFFrK50AH30ImiDA&sa=X&oi=translate&ct=result&resnum=3&ved=0CEAQ7gEwAg&prev=/search%3Fq%3DCisco%2BHCAP%26hl%3Des%26rlz%3D1R2RNTN_enEC381%26biw%3D1280%26bih%3D600%26prmd%3Divns, Guía de Implementación de Integración
- http://es.scribd.com/doc/57741341/T3-AAA, AAA
- http://www.cisco.com/go/ibns, Identidad Basada en Servicios de Red
- http://es.wikipedia.org/wiki/RADIUS, Protocolo RADIUS
- http://es.wikipedia.org/wiki/Network-attached_storage, Network-attached storage (NAS)
- http://www.cisco.com/en/US/docs/routers/access/1700/1701/software/configuration/guide/1700swcg.html, Guía de Configuración de Router Cisco, antiguo
- http://www.cisco.com/en/US/products/ps6406/index.html, Switch Cisco Catalyst 2960 Series
- http://es.wikipedia.org/wiki/Topolog%C3%ADa_de_red, Topologías de red
- http://www.eclac.org/noticias/paginas/3/20623/SeparataM_R.pdf, Redes de Seguridad Financiera e Integración regional
- http://platea.pntic.mec.es/~lmarti2/cableado.htm, Cableado estructurado
- http://ddd.uab.cat/pub/redes/15790185v11/Vol11_9.htm, La vida social de los routers
- http://www.slideshare.net/guest7bb5a1/redes-topologia-de-red, Topología de red
- http://www.cisco.com/en/US/products/ps5881/index.html, Router Integrado Cisco 2811
- http://www.gilisoft.com/product-usb-lock.htm, Gilisoft Lock
- http://www.monografias.com/trabajos28/manual-redes/manual-redes.shtml#determin, Manual para el Diseño de Redes LAN
- http://agile.inntegra.eu/metodologia/dimension-proyecto/a8-personas-roles-y-perfiles, Roles y Perfiles
- http://www.monografias.com/trabajos30/seguridad-redes/seguridad-redes.shtml#mejores, Seguridad en Redes en Computadoras
- http://www.cisco.com/web/ES/solutions/smb/products/routers_switches/catalyst_2960_series_switches/index.html#~overview, Switches CISCO Catalyst Series 2960
- http://es.hardware.com/tienda/cisco/WS-C3560G-48TS-S/refurbished/, Switches Cisco Catalyst 3560-48TS-S

- http://telematica.cicese.mx/seguridad/poli-segu.pdf, Política Oficial de Seguridad Informática del CICISE
- http://networkeando.blogspot.com/2009/01/configurando-aaa-en-un-router.html, Configurando AAA en un Router
- http://www.ciao.es/Cisco_Catalyst_3560G_48TS_48__637607, Cisco Catalyst 3560G-48TS 48
- http://technet.microsoft.com/es-es/library/cc737807%28WS.10%29.aspx, Protocolo de autenticación de contraseña
- http://technet.microsoft.com/es-es/library/cc785956%28WS.10%29.aspx, Protocolo de autenticación por desafío mutuo de Microsoft (MS-CHAP)
- http://technet.microsoft.com/es-es/library/cc758984%28WS.10%29.aspx, Protocolo MS-CHAP
- http://technet.microsoft.com/es-es/library/cc787927%28WS.10%29.aspx, Protocolo de autenticación por desafío mutuo de Microsoft versión 2 (MS-CHAP v2)
- http://technet.microsoft.com/es-es/library/cc739678(WS.10), Protocolo MS-CHAP versión 2
- http://technet.microsoft.com/es-es/library/cc782159%28WS.10%29.aspx, Protocolo de autenticación extensible (EAP)
- http://technet.microsoft.com/es-es/library/cc782851%28WS.10%29.aspx, Protocolo EAP
- http://es.wikipedia.org/wiki/Hash, Función Hash
- http://es.scribd.com/doc/40359306/A-a-A, Introducción AAA
- http://www.rediris.es/cert/doc/docu_rediris/recomendaciones/html/recomendaciones-node4.html, Seguridad en Nivel de Red

8. Biografía:

Daniel Martín Lescano Rodríguez nace el 11 de Abril de 1984 en la ciudad de Ambato, realizó sus estudios primarios en la Unidad Educativa La Salle, siguiendo sus estudios en el colegio particular San Alfonso obteniendo el título de Bachiller en Físico-Matemático. Actualmente terminando su carrera universitaria en Ingeniería Electrónica y Telecomunicaciones.